



SPYWOLF

Security Audit Report

(TESTNET)



Completed on
May 3, 2023

@SPYWOLFNETWORK



@SPYWOLFNETWORK



SPYWOLF.CO





OVERVIEW

This audit has been prepared for **PEPECHAIN** to review the main aspects of the project to help investors make an informative decision during their research process.

You will find a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

“

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

”





TABLE OF CONTENTS

Project Description	01
Contract 1 Information	02
Current Stats	03-04
Featured Wallets	05
Vulnerability Check	06
Threat Levels	07
Found Threats	08-A/08-C
Good Practices	09
About SPYWOLF	10
Disclaimer	11



PEPECHAIN

PROJECT DESCRIPTION

According to their whitepaper:

No whitepaper/website found

Release Date: Presale starts in May, 2023

Category: Meme token

01



CONTRACT INFO

Token Name
PEPE CHAIN

Symbol
PEPC

Contract Address
0x90C1dfcd094e378AA88f9274c0A10306640d681E

Network
Binance Smart Chain

Language
Solidity

Deployment Date
May 03, 2023

Verified?
Yes

Total Supply
420,000,000,000,000

Status
Not launched

TAXES

Buy Tax
none

Sell Tax
none

*Taxes can be changed in future



Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat



CURRENT STATS

(As of May 03, 2023)



Liquidity

Not added yet



Burn

No burnt tokens

Status:
Not Launched!

MaxTxAmount
12,600,000,000,000

LP Address(es)

Liquidity not added yet



TOKEN TRANSFERS STATS

Transfer Count	1
Uniq Senders	1
Uniq Receivers	1
Total Amount	99999.999999999999 FLY
Median Transfer Amount	99999.999999999999 FLY
Average Transfer Amount	99999.999999999999 FLY
First transfer date	2022-06-02
Last transfer date	2022-06-02
Days token transferred	1

SMART CONTRACT STATS

Calls Count	1
External calls	1
Internal calls	0
Transactions count	1
Uniq Callers	1
Days contract called	1
Last transaction time	2022-06-02 09:12:42 UTC
Created	2022-06-02 09:12:42 UTC
Create TX	0xd967d28dd785cee9f87d85850493ba161e75136a2ebe3b3598c37e325f65cfa5
Creator	0x740c39215fc735c0ac66672c54ab958594f9109d



VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed



THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.



FOUND THREATS

⚠ Medium Risk

Owner can set protections contract once, before trading is enabled.

Owner can set anti bots criteria in the protections contract.

The protections external contract is used to perform checks on regular users with each token buy/sell/transfer.

If protections contract is not set, unexcluded users from limitations won't be able to buy/sell the token.

The protections contract that perform these checks is not in the scope of the current audit.

```
function setInitializer(address initializer) external onlyOwner {
    require(!tradingEnabled);
    require(initializer != address(this), "Can't be self.");
    protections = Protections(initializer);
}

function setProtectionSettings(bool _antiSnipe, bool _antiBlock) external onlyOwner {
    protections.setProtections(_antiSnipe, _antiBlock);
}

function finalizeTransfer(address from, address to, uint256 amount,
bool buy, bool sell, bool other) internal returns (bool) {
    if (_hasLimits(from, to)) { bool checked;
        try protections.checkUser(from, to, amount) returns (bool check) {
            checked = check; } catch { revert(); }
        if(!checked) { revert(); }
    }
    .....
}
```



Informational

Owner can exclude address from fees, max transaction and max wallet limits. Such limits won't apply on excluded addresses.

```
function setExcludedFromLimits(address account, bool enabled) external onlyOwner {
    _isExcludedFromLimits[account] = enabled;
}

function setExcludedFromProtection(address account, bool enabled) external onlyOwner {
    _isExcludedFromProtection[account] = enabled;
}

function setExcludedFromFees(address account, bool enabled) public onlyOwner {
    _isExcludedFromFees[account] = enabled;
}
```

Owner can set max wallet size but cannot lower it than 1% of total supply. This is the maximum amount of tokens which single address can hold.

```
function setMaxWalletSize(uint256 percent, uint256 divisor) external onlyOwner {
    require((_tTotal * percent) / divisor >= (_tTotal / 100),
        "Max Wallet amt must be above 1% of total supply.");
    _maxWalletSize = (_tTotal * percent) / divisor;
}
```

Owner can change max transaction limit but it cannot be set below 0.5% of total supply.

```
function setMaxTxPercent(uint256 percent, uint256 divisor) external onlyOwner {
    require((_tTotal * percent) / divisor >= (_tTotal * 5 / 1000),
        "Max Transaction amt must be above 0.5% of total supply.");
    _maxTxAmount = (_tTotal * percent) / divisor;
}
```



Informational

Owner can set buy/sell/transfer fees up to 10%.

Combined buy+sell = 20%.

When fees are above 0, there will be certain amount of tokens that will be deducted from every transaction that users make. Deducted amount will be as much as the fees % from total amount that user had bought, sold and/or transferred.

```
uint256 constant public maxBuyTaxes = 1000;
uint256 constant public maxSellTaxes = 1000;
uint256 constant public maxTransferTaxes = 1000;
uint256 constant masterTaxDivisor = 10000;

function setTaxes(uint16 buyFee, uint16 sellFee, uint16 transferFee) external onlyOwner {
    require(!taxesAreLocked, "Taxes are locked.");
    require(buyFee <= maxBuyTaxes
        && sellFee <= maxSellTaxes
        && transferFee <= maxTransferTaxes,
        "Cannot exceed maximums.");
    _taxRates.buyFee = buyFee;
    _taxRates.sellFee = sellFee;
    _taxRates.transferFee = transferFee;
}
```

Owner can withdraw any tokens from the contract until liquidity is added. Once liquidity is added, the owner can withdraw any tokens from the contract with exception of the native blockchain token (ETH/BNB) and the native contract token (PEPC).

```
function sweepContingency() external onlyOwner {
    require(!_hasLiqBeenAdded, "Cannot call after liquidity.");
    payable(_owner).transfer(address(this).balance);
}

function sweepExternalTokens(address token) external onlyOwner {
    if (_hasLiqBeenAdded) {
        require(token != address(this), "Cannot sweep native tokens.");
    }
    IERC20 TOKEN = IERC20(token);
    TOKEN.transfer(_owner, TOKEN.balanceOf(address(this)));
}
```



RECOMMENDATIONS FOR

GOOD PRACTICES

1

Consider fundamental tradeoffs

2

Be attentive to blockchain properties

3

Ensure careful rollouts

4

Keep contracts simple

5

Stay up to date and track development

PEPE CHAIN

GOOD PRACTICES FOUND

- ✓ The owner cannot mint new tokens after deployment
- ✓ The owner can set a transaction limit, but can't lower it than 0.5% of total supply



SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 500 SUCCESSFUL CLIENTS
- ✓ MORE THAN 1000 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE



[SPYWOLF.CO](https://spywolf.co)



[SPYWOLF.NETWORK](https://spywolf.network)



[@SPYWOLFNETWORK](https://t.me/SPYWOLFNETWORK)



[@SPYWOLFOFFICIAL](https://t.me/SPYWOLFOFFICIAL)



[@SPYWOLFNETWORK](https://twitter.com/SPYWOLFNETWORK)



[@SPYWOLFNETWORK](https://github.com/SPYWOLFNETWORK)



Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.